

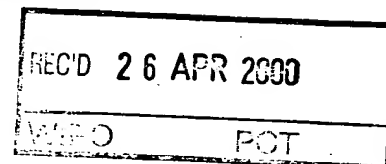


PCT/FR 00 / 0 0 6 7 9

GJU

# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION



## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 12 AVR. 2000

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

## DOCUMENT DE PRIORITE

PRESENTE OU TRANSMIS  
CONFORMEMENT A LA REGLE  
17.1.a) OU b)

INSTITUT  
NATIONAL DE  
LA PROPRIETE  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint Petersburg  
75800 PARIS Cédex 08  
Téléphone : 01 53 04 53 04  
Télécopie : 01 42 93 59 30

**THIS PAGE BLANK (USPTO)**

## REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

INPI  
INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08  
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Réservé à l'INPI

DATE DE REMISE DES PIÈCES

17 03 99

N° D'ENREGISTREMENT NATIONAL

99 03330

DÉPARTEMENT DE DÉPÔT

75

DATE DE DÉPÔT

17 MARS 1999

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE  
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

SCHLUMBERGER SYSTEMES

50 Av. Jean Jaurès - B.P 620-04  
92542 MONTROUGE CEDEX

A l'attention de Didier LEMOYNE

n° du pouvoir permanent références du correspondant téléphone

PG7390 76.0569 01 47 46 63 25

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention☐ demande divisionnaire☐ certificat d'utilité☐ transformation d'une demande  
de brevet européen

demande initiale

☐ brevet d'invention☐ certificat d'utilité n°

date

Établissement du rapport de recherche

☐ différé☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance

☐ oui☒ non

Titre de l'invention (200 caractères maximum)

DISPOSITIF D'AUTHENTIFICATION D'UN MESSAGE LORS D'UNE OPERATION DE TRAITEMENT  
CRYPTOGRAPHIQUE DUDIT MESSAGE

3 DEMANDEUR (S)

n° SIREN

code APE-NAF

Norm et prénoms (souligner le nom patronymique) ou dénomination

Schlumberger Systèmes

Forme juridique

Société Anonyme

Nationalité (s)

Adresse (s) complète (s)

Française

Pays

50, Avenue Jean Jaurès  
92120 MONTROUGE

France

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs

☐ oui☒ non

Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES

☐ requise pour la 1ère fois☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

SANS

7 DIVISIONS

antérieures à la présente demande n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE

(nom et qualité du signataire - n° d'inscription)

Didier LEMOYNE  
Mandataire (PG7390)

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Petersbourg

75800 Paris Cédex 08

Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

76.0569

N° D'ENREGISTREMENT NATIONAL

*PG 3330*

TITRE DE L'INVENTION :

DISPOSITIF D'AUTHENTIFICATION D'UN MESSAGE LORS D'UNE OPERATION DE TRAITEMENT  
CRYPTOGRAPHIQUE DUDIT MESSAGE

LE(S) SOUSSIGNÉ(S)

**Didier LEMOYNE**  
**SCHLUMBERGER SYSTEMES**  
50, avenue Jean Jaurès - BP 620-04  
92542 MONTROUGE CEDEX

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

**FAUSSE Arnaud.**  
11 bis rue de Maubeuge  
75009 PARIS  
France

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Le 17 mars 1999

*Didier Lemoigne*  
**Didier LEMOYNE**  
**(PG7390)**

**DISPOSITIF D'AUTHENTIFICATION D'UN MESSAGE LORS D'UNE  
OPERATION DE TRAITEMENT CRYPTOGRAPHIQUE DUDIT  
MESSAGE**

5        La présente invention concerne un dispositif d'authentification d'un message lors d'une opération de traitement cryptographique dudit message.

10        L'invention trouve une application particulièrement avantageuse dans le domaine des télécommunications par transmission de messages sous forme de fichiers électroniques.

15        Le développement des télécommunications par échange à distance de fichiers électroniques (commerce électronique, courrier électronique, notariation sous format électronique, etc) a provoqué l'avènement des technologies de traitement cryptographique dont le but est de sécuriser les messages transmis sur les réseaux de communication électronique face notamment aux attaques frauduleuses dont ils peuvent faire l'objet.

20        Parmi les opérations de traitement cryptographique d'un message, on peut citer le cryptage du message lui-même, dans sa totalité. Cependant, cette technique reste très lourde et souvent superflue, au moins dans les situations où le destinataire du message souhaite seulement s'assurer de l'identité de l'expéditeur et de l'intégrité du message qu'il reçoit en clair. C'est pour répondre à ces besoins qu'à été développé le concept de la signature électronique.

25        La signature électronique repose sur les principes suivants :

-        L'auteur d'un message qui souhaite en authentifier l'origine, c'est-à-dire le signer, dispose d'un nombre secret, appelé clé privée Kpr, destiné à élaborer une signature électronique pour ledit message. Une autre clé, dite clé publique Kpu, est disponible à tout destinataire d'un message en provenance du même expéditeur de manière à pouvoir  
30        vérifier la signature électronique du message reçu. Ladite clé publique est généralement associée au nom de l'expéditeur et à d'autres données,

durée de validité de la clé par exemple, dans une structure sécurisée appelée certificat. La sécurisation du certificat repose sur le fait que l'ensemble des données est lui-même signé par un « tiers de confiance » avec sa clé privée Kprtc et dont la clé publique Kputc est accessible à tous.

- L'élaboration de la signature se déroule en deux étapes. Tout d'abord, le message est réduit, on dit aussi « haché », au moyen d'un algorithme de réduction à sens unique, tels que ceux connus sous les noms de SHA1 ou MD5. Ensuite, le message ainsi réduit est crypté par un algorithme à clé publique, RSA, ECC par exemple, au moyen de la clé privée du signataire. Le résultat de ce cryptage constitue la signature.

- Le message en clair, la signature et, éventuellement, le certificat contenant la clé publique Kpu, sont envoyés au destinataire à travers le réseau de communication.

- Le destinataire doit alors vérifier que la signature reçue correspond bien au message et à son auteur. Pour cela, il réduit le message au moyen de l'algorithme de réduction à sens unique choisi par le signataire et décrypte la signature en utilisant la clé publique Kpu du signataire. La signature est reconnue valide si le résultat de la réduction du message est égal au résultat du décryptage de la signature. Le même procédé peut être utilisé pour vérifier les données contenues dans le certificat à l'aide de la clé publique Kputc du tiers de confiance qui l'a émis.

Il est intéressant de noter que la signature électronique est fonction du contenu du message et de la clé privée du signataire alors que la signature manuscrite identifie l'auteur mais est indépendante du message.

Afin de donner une valeur légale à la signature électronique, il est nécessaire de prouver certains faits. Entre autres :

- Le signataire doit disposer d'une clé privée dont personne d'autre ne dispose ;

- Le signataire doit être sûr du message qu'il signe ;
- Le destinataire doit être sûr que la vérification de signature est bien effectuée sur le message reçu ;
- Le destinataire doit être sûr du résultat de la vérification.

5 Si l'une des conditions ci-dessus n'est pas vérifiée, le signataire et/ou le destinataire peuvent contester la validité de la signature.

Or, la plupart des opérations de traitement cryptographique d'un message, notamment l'élaboration d'une signature électronique et sa vérification, sont effectuées dans les environnements informatiques de bureau. Cependant, les ordinateurs sont des systèmes ouverts sur  
10 lesquels il n'y a aucun contrôle de la sécurité, car l'utilisateur est libre d'installer tout logiciel de son choix. De même, pour les ordinateurs connectés aux réseaux de communication, de nombreux « virus » ou programmes non souhaitables peuvent être introduits à l'insu de  
15 l'utilisateur.

Il faut donc considérer l'environnement de l'ordinateur comme étant « non sûr ».

La situation la plus simple pour calculer une signature électronique, par exemple, pourrait consister à utiliser l'ordinateur  
20 comme moyen de stockage du message et des clés, et comme moyen d'élaboration de la signature. Cette solution est évidemment inacceptable car les clés stockées dans l'ordinateur peuvent être lues par un pirate à travers le réseau de communication et le même pirate pourrait utiliser à distance l'ordinateur pour calculer une signature sur  
25 un message que le propriétaire de l'ordinateur ne souhaiterait pas signer.

Il est donc souhaitable de pouvoir disposer d'un moyen sécurisé de traitement cryptographique qui, dans l'exemple de l'élaboration d'une signature, servirait au stockage de la clé privée du signataire et au  
30 calcul de la signature, le message restant stocké dans le moyen de stockage que constitue l'ordinateur par exemple.

Comme moyen sécurisé de traitement cryptographique, on peut utiliser une carte à microprocesseur, appelée aussi carte à puce. Dans le cadre de la signature d'un message, la carte à puce offre les services suivants :

- 5       - stockage de la clé privée du signataire ;
- calcul de la réduction du message ;
- cryptage du message réduit.

Un exemple typique d'architecture d'implantation de cette application comprend essentiellement un ordinateur auquel est  
10 connecté la carte à puce par l'intermédiaire d'un boîtier. Du point de vue informatique, les opérations se déroulent de la manière suivante :

- stockage du message dans un moyen de stockage de l'ordinateur ;
- édition du message sur l'ordinateur ;
- 15       - calcul du message réduit sur la carte à puce ;
- cryptage du message réduit par la carte, après vérification du code confidentiel introduit par le signataire au moyen du boîtier ;
- envoi du message et de la signature par la carte à l'ordinateur  
20       pour communication au réseau.

Avec ce système, le signataire est sûr que personne d'autre que lui ne peut utiliser sa clé privée pour signer. Cette solution est couramment utilisée et est suffisante pour un calcul de signature dont la portée ne vaut pas valeur légale, mais pour sécuriser un ensemble  
25 fermé d'ordinateurs, comme les réseaux internes de grandes entreprises.

Toutefois, on remarquera que le système de traitement cryptographique qui vient d'être décrit présente un certains nombres d'inconvénients :

- 30       - Le signataire n'est pas sûr du message qu'il signe puisqu'il n'est pas garanti qu'un virus dans l'ordinateur n'a pas modifié le message avant l'opération de réduction ;

- Le destinataire n'est pas sûr que la vérification est bien effectuée sur le message reçu puisqu'il n'est pas garanti qu'un virus dans l'ordinateur n'a pas fait apparaître le message correctement à l'écran alors que le message signé n'est pas celui visionné ;
- Le destinataire n'est pas sûr du résultat de la vérification puisqu'il n'est pas garanti qu'un virus dans l'ordinateur ne fait apparaître toute signature comme vérifiée alors qu'elle est fausse.

5  
10 Aussi, le problème technique à résoudre par l'objet de la présente invention est de proposer un dispositif d'authentification d'un message lors d'une opération de traitement cryptographique dudit message, comportant un moyen de stockage du message à traiter et un moyen sécurisé de traitement cryptographique dudit message, dispositif qui  
15 permette de remédier aux inconvénients des systèmes connus de traitement cryptographique, de manière à atteindre un niveau de sécurisation propre à conférer au message traité une valeur juridique incontestable.

20 La solution au problème technique posé consiste, selon la présente invention, en ce que ledit dispositif d'authentification comporte également un moyen de visualisation connecté directement audit moyen sécurisé de traitement cryptographique, le moyen sécurisé de traitement cryptographique étant apte à transmettre audit moyen de visualisation au moins le message reçu dudit moyen de stockage, lors de l'opération  
25 de traitement cryptographique.

Ainsi, on comprend qu'avec le dispositif d'authentification conforme à l'invention, l'opérateur effectuant le traitement cryptographique pourra avoir l'assurance que le message traité est bien authentique puisque, simultanément avec l'opération de traitement  
30 cryptographique, il verra apparaître sur le moyen de visualisation le texte du message en cours de traitement et ceci de façon indépendante

du moyen de stockage, ordinateur par exemple, susceptible d'attaque frauduleuse.

Selon un premier mode de réalisation du dispositif d'authentification conforme à l'invention, ladite opération de traitement  
5 cryptographique est une opération de signature dudit message, ledit moyen sécurisé de traitement cryptographique étant un moyen d'élaboration d'une signature. Dans ce cas, il est prévu que, l'élaboration de ladite signature comprenant une opération de réduction du message suivie d'une opération de cryptage du message réduit, ledit  
10 moyen d'élaboration d'une signature transmet le message à signer audit moyen de visualisation au fur et à mesure de l'opération de réduction.

Dans ce premier mode de réalisation, le message est visualisé au signataire qui va signer, avec l'assurance que le message qui va être signé n'aura pas été falsifié, la fonction de visualisation (impression,  
15 affichage ou archivage) étant un environnement fermé considéré comme « sûr ».

Selon un deuxième mode de réalisation du dispositif d'authentification conforme à l'invention, ladite opération de traitement  
20 cryptographique est une opération de vérification d'une signature dudit message, ledit moyen sécurisé de traitement cryptographique étant un moyen de vérification de signature. Dans ce cas, il est prévu que, ladite vérification de signature comprenant une opération de réduction du message et une opération de décryptage de ladite signature, ledit moyen de vérification de signature transmet le message à authentifier audit  
25 moyen de visualisation au fur et à mesure de l'opération de réduction.

Dans ce deuxième mode de réalisation, sont visualisés au destinataire le message et la signature sur lesquels la vérification de signature est effectuée, ainsi que le résultat de la vérification, et éventuellement le certificat, sans que ces éléments ne circulent dans le  
30 moyen de stockage, « non sûr ».

La description qui va suivre en regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma en perspective d'un dispositif d'authentification conforme à l'invention.

La figure 2 est bloc-diagramme du dispositif d'authentification de la figure 1.

Le dispositif d'authentification représenté sur la figure 1 est destiné à authentifier un message lors d'une opération de traitement cryptographique dudit message.

Dans la suite de cette description, on envisagera deux types de traitement cryptographique, à savoir la signature d'un message à envoyer à un destinataire et, inversement, la vérification par un destinataire de la signature d'un message reçu. Bien entendu, d'autres opérations de traitement cryptographique peuvent être mises en oeuvre au moyen de dispositif d'authentification de la figure 1, telles que le cryptage du message lui-même.

D'une manière générale, le dispositif d'authentification de message de la figure 1 comporte un moyen de stockage dudit message, constitué par exemple, par une mémoire dans l'unité centrale 11 d'un ordinateur 10. En fait, le message stocké est celui que l'auteur dudit message a composé au moyen du clavier 12 et qui doit faire l'objet d'une signature électronique. Normalement, le message composé apparaît sur l'écran 13 de l'ordinateur 10. L'unité centrale 11 communique avec l'extérieur, notamment avec les réseaux de communication, au moyen d'un câble 14 par lequel transitent les messages à signer et à envoyer ou les messages signés reçus.

L'unité centrale 11 est reliée par un câble 15 de liaison à un moyen sécurisé 21 de traitement cryptographique, ici constitué par une carte à microprocesseur disposée dans un boîtier 22. Comme le montre la figure 2, ledit boîtier 22 comprend un circuit 221 d'interface appelé circuit de commandes/données. Le message devant être signé ou le

message dont la signature doit être vérifiée, ainsi que les données nécessaires aux opérations de signature ou de vérification, arrivent du moyen 11 de stockage à la carte 21 à puce par ce circuit en respectant par exemple la norme ISO 7816. Le circuit 221 de commandes/données dispose d'une entrée permettant de recevoir en actionnant un bouton 222 un signal de déclenchement de l'opération de signature et les données sur un clavier 224 du boîtier, comme par exemple un code confidentiel.

D'autre part, la carte 21 à puce est connectée directement à un moyen 30 de visualisation, ici une imprimante mais qui pourrait être tout aussi bien un écran ou un moyen d'archivage, de manière à pouvoir transmettre au moins le message reçu de l'unité centrale 11, lors de l'opération du traitement cryptographique. La liaison entre la carte 21 à puce et l'imprimante 30 est réalisée par une interface 223 de visualisation du boîtier 22 par lequel passeront le message, et d'autres données devant être authentifiées.

L'architecture du dispositif d'authentification représentée aux figures 1 et 2 est donc basée sur une carte 21 à puce faisant le pont entre une zone « non sûre », l'ordinateur 10, et une zone « sûre », l'imprimante 30, la carte elle-même étant réputée « très sûre ».

Les entrées/sorties des circuits de commandes/données 221 et de visualisation 223 sont électriquement indépendantes lorsqu'aucune carte à puce n'est présente dans le boîtier 22. Lorsqu'une carte 21 est insérée dans le boîtier 22, la masse électrique est alors partagée entre les deux circuits 221 et 223. Les données issues de la carte 21 vers le circuit 223 de visualisation sortent par une sortie  $O_2$  spécifique et physiquement distincte de la sortie  $O_1$  utilisée pour le transfert des commandes/données. De même, les entrées  $I_1$  et  $I_2$  de commandes/données et de visualisation de la carte 21 sont physiquement distinctes. En fait, le seul lien logique entre les données circulant dans les circuits de commandes/données 221 et de visualisation 223 est le logiciel de la carte, réputé « très sûr ».

Dans le cas où la liaison entre la carte 21 à puce et l'imprimante 30 n'apparaîtrait pas suffisamment sécurisée, du fait notamment de son cheminement, il est prévu que la carte 21 puisse transmettre à l'imprimante 30 le message à traiter, et d'autres données, sous forme cryptée. Le mécanisme utilisé sera par exemple un algorithme symétrique, comme le triple DES, dont la clé peut être fixée ou négociée entre la carte 21 et le moyen 30 de visualisation.

Le déroulement d'une opération de signature d'un message est le suivant :

- 10        1. Le message à signer est édité dans le moyen 11 de stockage de l'ordinateur 10 et, éventuellement apparaît sur l'écran 13, puis le signataire demande à l'ordinateur de démarrer l'opération de signature.
2. L'ordinateur 10 transmet le message à la carte 21 via le circuit 221 de commandes/données par paquets de N octets afin d'être réduit par un algorithme de hachage (N = 64 si l'algorithme SHA1 est employé).
- 15        3. Lors de l'initialisation de l'algorithme de hachage, le logiciel 211 de la carte 21 envoie une commande d'initialisation du moyen 30 de visualisation qui permettra d'authentifier le message de manière sûre.
- 20        4. Lors de l'arrivée du message venant du moyen 11 de stockage, le logiciel 211 de la carte 21 en calcule en ligne la réduction et le recopie sur la sortie 02 de visualisation, si bien que le moyen 30 de visualisation pourra faire apparaître, ici imprimer, le message au fur et à mesure de l'opération de réduction.
- 25        5. Lorsque la totalité du message a été envoyée à la carte 21 à puce par l'ordinateur, et avant d'effectuer l'opération de cryptage du message réduit, la carte se met en attente de réception d'un message de commande.
6. Le signataire a le temps d'authentifier le message imprimé, puis, s'il en accepte le contenu, compose ledit message de commande sous forme d'un code confidentiel saisi sur le clavier 224 du boîtier 22. Le circuit 221 de commandes/données génère lui-même la commande de
- 30

l'opération de cryptage du message réduit en présentant la commande et le code confidentiel entré sur le clavier 224 par le signataire. L'ordinateur ne peut pas voir le contenu de cette commande. On pourra aussi disposer d'une entrée physiquement distincte sur la carte 21 à puce pour rentrer le code confidentiel.

7. La carte 21 à puce calcule la signature, renvoie la valeur à l'ordinateur 10 et, au besoin, au moyen 30 de visualisation. Le logiciel 211 de la carte 21 pourra aussi inclure d'autres données à visualiser, telles que et non limitativement le numéro de série de la carte, le nom du signataire, etc, si ces données sont présentes dans la carte 21.

Il est important de noter que l'opération de signature ne pourra être activée sur la carte 21 que suite à une réduction et l'entrée du code confidentiel en tant que message de commande du cryptage du message réduit. De plus, suite au calcul de signature, l'autorisation de signature est effacée, obligeant ainsi à entrer le code confidentiel volontairement pour toute opération de signature ultérieure.

S'agissant d'une opération de vérification de la signature d'un message, le message et sa signature sont envoyés au destinataire, dans l'unité centrale 11 de son ordinateur 10. Le destinataire désirera alors vérifier l'authenticité de la signature par rapport au message et au signataire. On se placera ici dans le cas où le certificat du signataire est également envoyé au destinataire.

Le destinataire doit effectuer deux types de vérification. D'une part, la vérification du lien entre l'identité du signataire et la clé publique de vérification, c'est-à-dire la vérification du certificat, et, d'autre part, la vérification de la valeur de la signature par rapport au message reçu et au certificat.

La séquence se déroule comme suit:

1. Le destinataire déclenche l'opération de vérification par le chargement dans la carte 21 à puce du certificat du signataire et de la clé publique du tiers de confiance qui a issu le certificat.

2. L'ordinateur 10 demande la vérification du certificat avec la clé publique du tiers de confiance. Cette commande déclenche l'initialisation du moyen 30 de visualisation par la carte.
3. La carte 21 vérifie le certificat et transmet au moyen 30 de visualisation, via le circuit 223 de visualisation, les données suivantes: validité du certificat (avec les dates), clé publique du tiers de confiance utilisée pour vérifier le certificat, clé publique du signataire, nom du signataire, et d'autres données pouvant être liées au contexte d'utilisation. Ainsi, un destinataire recevant un faux certificat, numériquement intègre mais issu par un faux tiers de confiance, s'en apercevrait d'une manière sûre en comparant la valeur visualisée de la clé publique du «faux tiers» avec celle du «vrai tiers» dont la clé publique est publiée notoirement.
4. Lorsque le certificat est vérifié, l'ordinateur 10 déclenche la commande de l'opération de réduction et envoie le message à la carte 21.
5. Lors de l'arrivée du message venant du moyen 11 de stockage, le logiciel 211 de la carte en calcule en ligne la réduction et le recopie sur la sortie O<sub>2</sub> de visualisation, si bien que le moyen 30 de visualisation fera apparaître, ici imprimer, le message au fur et à mesure de l'opération de réduction.
6. Lorsque la totalité du message a été envoyée à la carte 21 à puce par l'ordinateur 10, ce dernier demande alors la vérification de signature. Il passe en paramètre la valeur de la signature reçue du signataire. Le logiciel 211 de la carte déchiffre la signature avec la clé publique du signataire et la compare avec le résultat de la réduction effectuée en étape 5. S'il y a égalité, la carte 21 envoie un message à l'ordinateur 10, indiquant que la signature est conforme au message et à la clé publique du certificat présenté. La carte envoie au circuit 223 de visualisation le message «Signature OK. Fin de vérification»,

qui est visible par le vérificateur. Si la signature n'est pas exacte, alors la carte envoie un message à l'ordinateur, indiquant que la signature est non conforme au message ou à la clé publique du certificat présenté. La carte envoie au circuit 223 de visualisation le message «Signature inexacte. Fin de vérification», qui est visible par le vérificateur.

L'ensemble de ces actions doit se dérouler dans l'ordre indiqué sans incident, sinon, la séquence est annulée par la carte 21 à puce et il est nécessaire de tout recommencer.

## REVENDICATIONS

- 5           1. Dispositif d'authentification d'un message lors d'une opération  
de traitement cryptographique dudit message, comportant un  
moyen (11) de stockage du message à traiter et un moyen  
sécurisé (21) de traitement cryptographique dudit message,  
caractérisé en ce que ledit dispositif d'authentification comporte  
10 également un moyen (30) de visualisation connecté directement  
audit moyen sécurisé (21) de traitement cryptographique, le  
moyen sécurisé (21) de traitement cryptographique étant apte à  
transmettre audit moyen (30) de visualisation au moins le  
message reçu dudit moyen (11) de stockage, lors de l'opération  
de traitement cryptographique.
- 15           2. Dispositif d'authentification selon la revendication 1, caractérisé  
en ce que ledit moyen sécurisé (21) de traitement  
cryptographique est apte à transmettre audit moyen (30) de  
visualisation le message à traiter sous forme cryptée.
- 20           3. Dispositif d'authentification selon l'une des revendications 1 ou  
2, caractérisé en ce que ledit moyen sécurisé (21) de traitement  
cryptographique est constitué par une carte à microprocesseur  
disposée dans un boîtier (22) connecté, d'une part, audit moyen  
(11) de stockage, et, d'autre part, audit moyen (30) de  
visualisation.
- 25           4. Dispositif d'authentification selon l'une quelconque des  
revendications 1 à 3, caractérisé en ce que ledit moyen (30) de  
visualisation est une imprimante, un écran ou un moyen  
d'archivage.
- 30           5. Dispositif d'authentification selon l'une quelconque des  
revendications 1 à 4, caractérisé en ce que ladite opération de  
traitement cryptographique est une opération de cryptage dudit  
message.

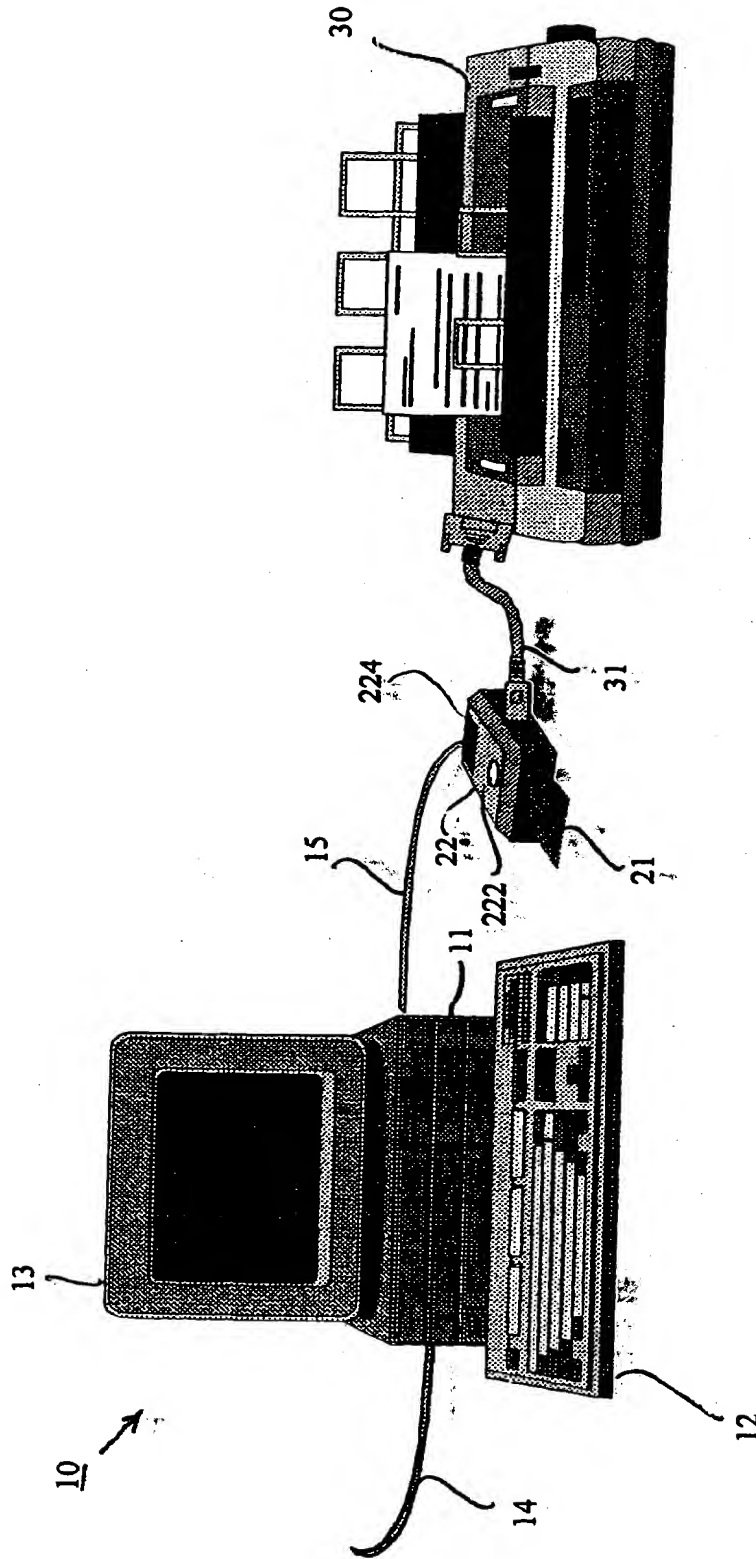
- 5 6. Dispositif d'authentification selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ladite opération de traitement cryptographique est une opération de signature dudit message, ledit moyen sécurisé (21) de traitement cryptographique étant un moyen d'élaboration d'une signature.
- 10 7. Dispositif d'authentification selon la revendication 6, caractérisé en ce que, l'élaboration de ladite signature comprenant une opération de réduction du message suivie d'une opération de cryptage du message réduit, ledit moyen (21) d'élaboration d'une signature transmet le message à signer audit moyen (30) de visualisation au fur et à mesure de l'opération de réduction.
- 15 8. Dispositif d'authentification selon la revendication 7, caractérisé en ce que l'opération de cryptage est effectuée après l'opération de réduction sur réception par le moyen (21) d'élaboration d'une signature d'un message de commande.
- 20 9. Dispositif d'authentification selon la revendication 8, caractérisé en ce que ledit message de commande est un code confidentiel.
- 10 10. Dispositif d'authentification selon l'une quelconque des revendications 6 à 9, caractérisé en ce que ledit moyen (21) d'élaboration d'une signature transmet également audit moyen (30) de visualisation des données relatives à l'élaboration de la signature.
- 25 11. Dispositif d'authentification selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ladite opération de traitement cryptographique est une opération de vérification d'une signature dudit message, ledit moyen sécurisé (21) de traitement cryptographique étant un moyen de vérification de signature.
- 30 12. Dispositif d'authentification selon la revendication 11, caractérisé en ce que, ladite vérification de signature comprenant une opération de réduction du message et une opération de décryptage de ladite signature, ledit moyen (21) de

vérification de signature transmet le message à authentifier audit moyen (30) de visualisation au fur et à mesure de l'opération de réduction.

5      **13.** Dispositif d'authentification selon la revendication 12, caractérisé en ce que, ledit message étant accompagné d'un certificat de signature, ledit moyen (21) de vérification de signature effectue également une opération de vérification dudit certificat.

10      **14.** Dispositif d'authentification selon la revendication 13, caractérisé en ce que, ledit moyen (21) de vérification de signature transmet également audit moyen (30) de visualisation des données dudit certificat et des résultats de la vérification.

15



**Figure 1**

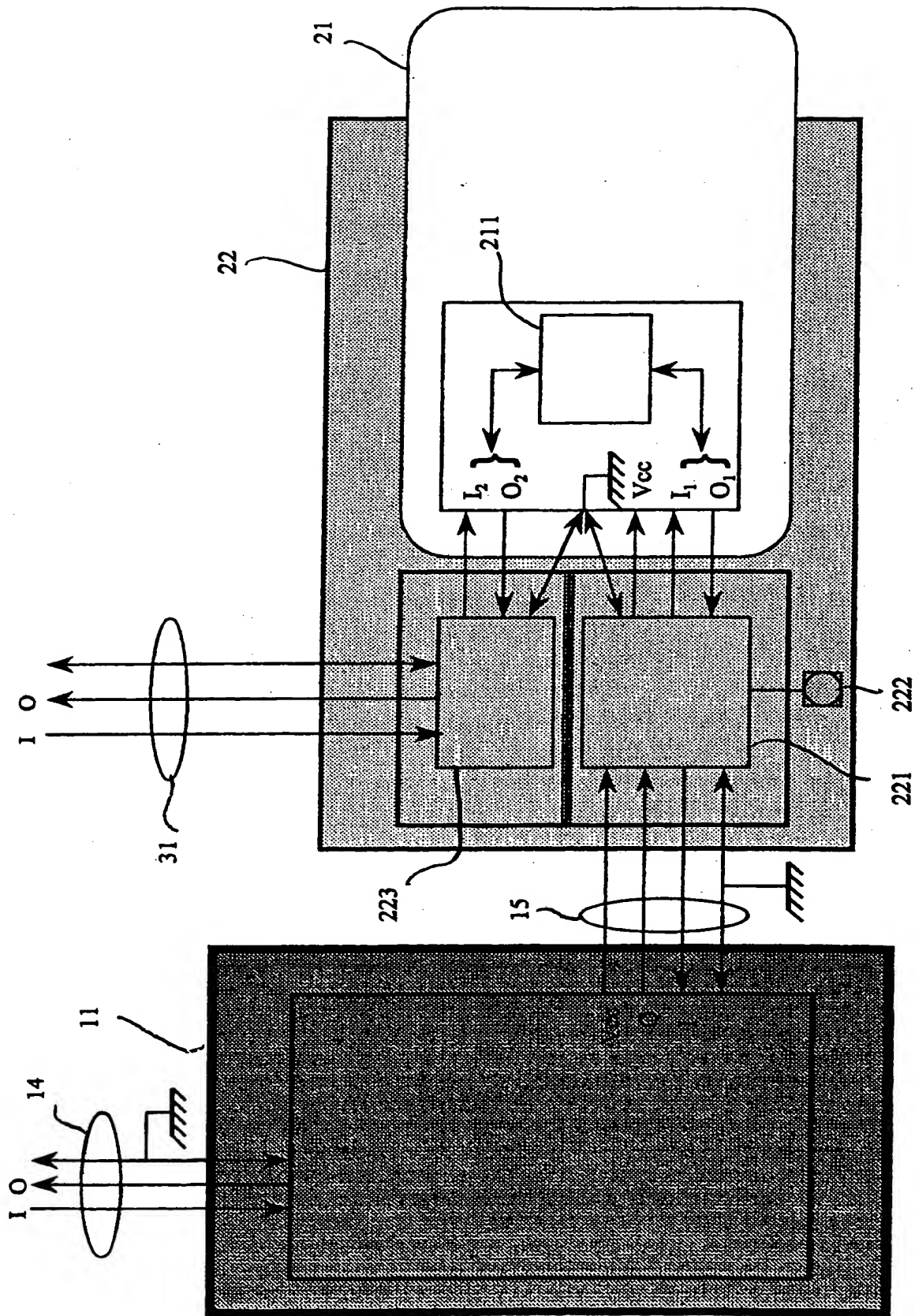


Figure 2

- 5 1. Dispositif d'authentification d'un message émis par un signataire et reçu par un destinataire, comportant un moyen (11) de stockage du message reçu et un moyen sécurisé (21) de traitement cryptographique dudit message, caractérisé en ce que ledit dispositif d'authentification comporte également un moyen (30) de visualisation connecté directement audit moyen sécurisé (21) de traitement cryptographique, le moyen sécurisé (21) de traitement cryptographique étant apte à transmettre  
10 audit moyen (30) de visualisation au moins un message reçu dudit moyen (11) de stockage, lors d'une opération de traitement cryptographique, ledit moyen sécurisé (21) de traitement cryptographique étant un moyen de vérification de  
15 signature du message reçu.
2. Dispositif d'authentification selon la revendication 1, caractérisé en ce que ledit moyen sécurisé (21) de traitement cryptographique est constitué par une carte à microprocesseur disposée dans un boîtier (22) connecté, d'une part, audit moyen  
20 (11) de stockage, et, d'autre part, audit moyen (30) de visualisation.
3. Dispositif d'authentification selon l'une quelconque des revendications 1 à 2, caractérisé en ce que ledit moyen (30) de visualisation est une imprimante, un écran ou un moyen  
25 d'archivage.
4. Dispositif d'authentification selon l'une quelconque des revendications précédentes, caractérisé en ce que ladite opération de traitement cryptographique est une opération de vérification d'une signature dudit message.
- 30 5. Dispositif d'authentification selon la revendication 4, caractérisé en ce que, ladite vérification de signature comprenant une opération de réduction du message et une opération de

décryptage de ladite signature, ledit moyen (21) de vérification de signature transmet le message à authentifier audit moyen (30) de visualisation au fur et à mesure de l'opération de réduction.

- 5      6. Dispositif d'authentification selon la revendication 5, caractérisé en ce que, ledit message étant accompagné d'un certificat de signature, ledit moyen (21) de vérification de signature effectue également une opération de vérification dudit certificat.
- 10     7. Dispositif d'authentification selon la revendication 6, caractérisé en ce que, ledit moyen (21) de vérification de signature transmet également audit moyen (30) de visualisation des données dudit certificat et des résultats de la vérification.

**THIS PAGE BLANK (USPTO)**